Volume 18, Issue 32 Atari Online News, Etc. August 12, 2016

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1832 08/12/16

~ Google Wants Flash Gone ~ WWW Silver Jubilee! ~ High-speed Internet

-* Blackhat Firm Offers Bounty! *-
-* Oracle’s MICROS Systems Get Hacked! *-
-* New Hack Uses Hard Drive’s Noise To Steal! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"

Go USA! Yes, the U.S. Olympic teams are doing very well in Rio, although there have been a few "disappointments" along the way. These athletes have been doing an incredible job and have a lot of accomplishments in which to be proud!

The heat waves continue here in the Northeast; and they have been brutal! Added to the heat has been the oppressive humidity. Our air conditioning units have been running most of the day for quite some time. It’s been so humid that the condensation unit on our mobile unit has filled up 2-3 times a day - something we’ve never had to worry about in the past few years! Usually during this time of the year, and weather, we get numerous thunderstorms which bring quite a bit of rain. Not so this year. What little rain we’ve received has been for a very brief period, if at all. In my area, we’ve reached what has been classified as "Extreme Drought" conditions. The only "green" spots in my lawn are the sparse patches of crab grass! I think the last time that I mowed my lawn was in early June!

Well, while we try to find a good way to stay cool here, I hope that you’re all finding your weather a bit more tolerable! Stay cool and hydrated!

Until next time...

=~=~=~=

Frogger STFM/E BETA Release

Updated version, almost complete..

SYS REQS

ATARI STFM/STE (TOS 2.06 Compatible)
1Mb of Memory or more
Colour Television/Monitor

N.B This version is NOT Falcon/TT/HADES compatible, its unlikely the actual game will be either. The game was always developed for the STFM/E range and this has stayed true right up until the very end. I would have hoped it was 030 compatible without too much issue but as a one-man operation it is far too time consuming to fix a game for machines I’ll never use/own.

Please feel free to Fix it yourself if you have the necessary skills ;) I’d always appreciate it !!

Two differing formats for your enjoyment. They are NOT different versions so just download the one you prefer.

Frogger MSA Disk Image:
http://www.atari-forum.com/download/file.php?id=29812
(251.47 KiB)

Frogger Files for HDD:
http://www.atari-forum.com/download/file.php?id=29813
(37.12 KiB)

Now go play :D

=~=~=~=

->In This Week’s Gaming Section - Sony s PlayStation Neo Expected Next Month!
""""""""""""""""""""""""""""" Nintendo Confirms NES Classic Mini Features!

Nintendo Wanted Gambling!
And more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Sony s PlayStation Neo Expected To Debut September 7

Sony s PlayStation Neo (also sometimes called the PlayStation 4.5 or PlayStation 4K) has been a hot topic since rumors of its existence started spreading earlier this spring. Sony is expected to unveil its mid-cycle upgrade platform in just under a month, at a special press event held in New York City. Sony supposedly chose the September 7 date to avoid going directly up against Nintendo s anticipated announcement of its NX platform at the Tokyo Game Show on September 12.

This report, by French website Gameblog, confirms rumors we ve heard concerning the PS4 Neo s anticipated launch. Sony is rumored to want both the new platform and PlayStation VR to launch in time for Christmas 2016, and the resulting hardware extravaganza could contribute to significant earnings for the company   assuming customers bite.

The rumors we ve heard to date suggest that Sony will rigidly enforce backwards compatibility requirements for this new PS4. Games can t include all-new modes of play or Neo-specific features, though developers are allowed to enhance existing capabilities for the new platform. The new console will supposedly feature eight AMD Jaguar CPU cores clocked at 2.1GHz (a 31% improvement), a Polaris-derived GPU with double the GPU cores and a higher clock frequency (2,304 cores total and a 911MHz clock, up from 1,154 cores and 853MHz), and 218GB/s of memory bandwidth, up from 176GB/s on the PS4 standard.

That s all well and good, but it doesn t tell us much about actual game performance. While there are a number of differences between the PC ecosystem and its console counterpart, we should be able to draw some relative performance data by looking at our own AMD RX 480 review. While none of our desktop GPUs is an exact match for the PS4 or PS4 Neo, the R9 270X comes fairly close to the PS4, while the RX 480 isn t far off the PS4 Neo. In the graphs below, pay attention to just the 270X and the RX 480 those are the GPUs we re comparing against each other.

In two DX11 benchmarks and one DX12 test, we see the RX 480 blasting past the R9 270X. Again, we re not claiming that the PS4 Neo will be twice as fast as the PS4   the two platforms are simply too different to make that assertion. But the significant performance improvements to Polaris should have a correspondingly significant impact on the PS4 Neo s overall performance, and a 1.4   1.6x performance increase seems completely plausible.

The 31% increase in CPU clock speed will keep games from becoming CPU-limited, and it s possible that Sony addressed other issues in the SoC as well. The PS4 s SoC is better described as two quad-core chips than a single eight-core SoC, but Sony may have paid AMD to design a unified eight-core chip with a faster L2 cache (Jaguar s L2 historically runs at 50% CPU clock). Past presentations from developers like Naughty Dog have stated that looking up data in the other CPU cluster s L2 cache has a latency hit almost as severe as just pulling data from main memory in the first place; a unified eight-core chip would alleviate this problem and allow developers to multi-thread more effectively.

There s still no word on price or availability, but this new console could effectively sweep Microsoft s refreshed Xbox One S completely off the table. While the Xbox One S is slightly faster than the original model, it s not going to fare well against a revitalized PS4   not when those comparisons already tilt Sony s direction in the first place. Microsoft s Project Scorpio is expected to leapfrog the PS4 altogether, but that s not going to happen for another 12 months. If Sony s VR experience is strong, the company could be set to own 2017   news that s probably not particularly welcome at Nintendo, which is hoping to ignite fan interest around its own platform, the mobile/living room hybrid Nintendo NX.

Nintendo Confirms NES Classic Mini Has Several Display Modes, Instant Saves

One of the problems with trying to play games using a retro console such as a NES, SNES, or Genesis on a modern HD TV is that the games don t look great. That s why the XRGB mini has proved so popular as it solves the problem. It s also why the Retron 5 works so well because it also solves the display issue by default.

Thankfully, Nintendo has taken the time to ensure the NES games included with the forthcoming NES Classic Mini all look great on a HD TV. But that s not all. Julie Gagnon, communications manager at Nintendo of Canada, has given a French-language radio interview where she goes into more detail on the display options.

It seems the Classic Mini will be a lot like the Retron 5 in terms of the display options you have available. As well as a standard HD-resolution output, the tiny NES will allow you to simulate the look of the game as you would experience it on a CRT. There will also be a 4:3 mode and a pixel-perfect mode where every pixel is a perfect square. So that s all 30 games with multiple viewing options available.

Gagnon also commented on game saves. There will be permanent save points within each game, but Nintendo has also added instant temporary saves. That means you ll be able to stop playing at any point and return later without losing progress. The fact they are instant suggests the save may only last as long as the Classic Mini is powered on, where as the permanent saves are, well, permanent.

The Nintendo Classic Mini is set to go on sale on November 11 for $59.99 including 30 games and one NES controller.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

""""""""""""""""""""

When Nintendo Wanted To Bring Gambling Into American Homes

In 1988, Nintendo released a modem for its Famicom system in Japan. A crude device, it didn’t allow for online play; just some downloadable stuff and access to basic news and information services.

The device was never released in the United States, but it wasn’t for want of trying. Indeed, Nintendo figured at the time it had the perfect entry path for the add-on: the lottery.

The year was 1991, and with millions of Nintendo Entertainment

Systems spread across the US, Minneapolis-based company Control Data Corporation had a bright idea: combine the consoles with advancing online technology to bring not online gaming into the homes of Americans, but online gambling.

Nintendo jumped at the idea. As it would, seeing as it gave them another chance to stack something on top of something else! With the company designing a new modem (the Famicom ones wouldnt fit in a NES) and providing them free of charge, CDC also got the blessing of the State of Minnesota to trial a system where the NES could be used as a means for people to play the lottery from their living room.

The three parties planned to sign up 10,000 homes for the trial, and while Nintendo handed out free modems, in an even sweeter deal, Minnesota also handed out free NES consoles to those involved who didn't already have one.

For a monthly subscription fee of $10 (remember, that's 1991 money), users would also get a special cartridge for the NES that let them access the lottery, after which they could play every game that month, right up to and including the big jackpots.

Users could pick their own digits or, if they weren't feeling lucky, let the computer pick numbers for them. The lottery's interface was even "gamified", with some screens livened up with graphics like men fishing for numbers.

This of course didn't go down very well with many people, who realised the dangers of not just associating what was still a "children's" brand with an act restricted to adults, but of placing the means to gamble in a way kids could easily access it.

"Kids are gambling now; this will allow them to gamble more," Tony Bouza, a former Gaming Commissioner in Minnesota told the New York Times in 1991.

Bob Heitman, GM of the Sierra online gaming network (run by famed PC publishing house Sierra), told the paper "It's Jimmy the Greek comes home to your kid's bedroom."

"I have a bad feeling for lotteries. As a family game company, I would not do it or advocate that our company do it."

To counter this, Nintendo said that over one third of its NES users by 1991 were over the age of 18, while CDC pointed out the service would not only be password-protected, but that signing up would require certified copies of identification be sent and approved, and that there would also be a $50 daily limit on spending.

Not that any of that ended up mattering. The test went nowhere, scuppered before it could even begin by the complexity of the tech and political pressure, and despite plans for a national roll-out of the program, Nintendo quickly and quietly dropped the scheme. And wouldn't return to online technology for a long, long time.

Commodore 64 Receives Shotgun Four Player Deathmatch
Game Available Free and as Box Set

It is not often that we are alerted to new Commodore 64 games but when we do get these, we make sure to tell everyone we can about them. Why? For me it is simple, I love the Commodore 64 gaming computer. It is iconic and awesome, I mean, short of the NES name a console with as many fun games to play. Anyhow, Shotgun is a new four player deathmatch single screen game that was released in May of this year. I am writing about it now, first because I was just e-mailed about it, and second the publisher has released a boxed set for the game recently.

If you are wondering how in the world you are going to play four players in a game like Shotgun, it is simple. You will need the Protovision 4-Player Interface to plug in two additional controllers. If you don t have access to that accessory, nor care to purchase one, you can still play two player deathmatch in Shotgun. Playing two player seems like it would lend itself quite well to gamers that grew up playing the classics like Combat on the Atari 2600.

The big news here is, besides Shotgun being available as a free and legal download, is that the publisher has released a boxed set. In this boxed set you will receive the box, manual and a 5.25 disk with the game on it. They have not stopped there as for a short period longer there are three surprise items tucked into each boxed set. I say for a short time because it is still a surprise as no one has spoiled what those three extras are yet. There is no word on if those prizes will be limited to a certain number of copies sold or not.

If you are no longer rocking a Commodore 64 then you can grab Shotgun, legally, in digital format for use with emulators. Check out Shotgun while you can!

Update: From the developer we have learned that if you are playing Shotgun via the legally free digital files you can play four player mode using the Commodore 64 emulator, Vice. Just enable Userport Joystick Adapter in the settings.

Head over to shotgun.drwuro.com to get your copy today.

Rare Atari Find Was A Thrill

It was 1983, and like many kids his age, Doug Johnson was into Atari.

Connor Johnson of Kincardine, Ont., who is visiting friends and relatives in Truro, was looking for a copy of his father s favourite boyhood video game in a local collectibles shop.

Well, he had been. The 13-year-old s interests were shifting.

Doug was ready to move on and had his sights set on the next big thing in video technology   ColecoVision.

So, reluctantly, he took his entire collection of Atari games and sold them.

As we know, everything old is new again.

Connor, formerly of Valley and now living in Ontario, was home for a recent visit. And, he was on a quest.

He was looking for a vintage Atari game and couldn t believe his luck when he came across the one he was after at a Truro shop, Cooper s Cabin.

After all, chances of finding this game were pretty slim. And chances of what happened next would be considered astronomical.

 I was in shock, Connor said. I was speechless at first. I was agape.

That s understandable. Scribbled across the front of the tattered instruction booklet was Douglas Roy Johnson East Mountain.

That would be Connor s dad.

Inside the booklet are various other scribbles and underlined areas made more than three decades ago.

 He remembered doing all that. It all came back to him when I described it to him, said Connor, 22.

 He was elated because the chances of me getting it were already one in a million.

After seeing a picture of the manual and the game his son purchased, Doug confirmed there is no doubt.

 That was my instruction booklet and game, he said. That s definitely my scribbles.

Reached at his home in Kincardine, Ont., the elder Johnson admitted, it was quite shocking.

 I played that more than anything else, he said, of the Adventure version of Atari.

The odds had to be on par with winning the lottery. For Connor, it meant even more.

 To find my father s game and look through this and get a peek into his childhood, that means more to me than any amount of money will, he said. Because I got to look in here and see what 10-year-old Douglas Johnson   thought and what games he liked.

Doug is a manager of business intelligence (information technology) at the Bruce Nuclear Generating Station, near Kincardine.

And, to this day, he is still a video gamer.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Secretive Hacking Group May Be Linked to Espionage

A previously undetected, secretive group of hackers has been targeting organizations in Russia, China, and Europe since at least 2011, Reuters reported Monday.

Antivirus software maker Symantec in a Sunday blog post said the group, which it nicknamed "Strider," has developed advanced spyware programs to target "organizations and individuals that would be of interest to a nation state’s intelligence services."

The spyware they use is called Remsec, and includes modules that can load files from a disk or a network connection and execute them. It can also log keystrokes and create backdoors in HTTP code and parts of the Windows operating system.

"Based on the espionage capabilities of its malware and the nature of its known targets, it is possible that the group is a nation-state level attacker," Symantec wrote. The targets include multiple organizations and individuals in Russia, an airline in China, and an embassy in Belgium.

Symantec competitor Kaspersky said it first discovered evidence of the hacking group in September 2015. It named the group "Project Sauron," a reference to the the title character in The Lord of the Rings. Kaspersky claims that targets include scientific research centers, military facilities, and telecoms.

While antivirus protection provides some defense against the hacking group, its techniques appear specifically engineered to avoid detection.

"ProjectSauron’s tactics are designed to avoid creating patterns," Kaspersky explained in a blog post. "Implants and infrastructure are customized for each individual target and never re-used   so the standard security approach of publishing and checking for the same basic indicators of compromise (IOC) is of little use."

Looks Like a Russian Cybergang Hacked Into One of the World s Largest Payment Systems

According to a report by security blogger Brian Krebs, Oracle s popular MICROS point-of-sale terminals support website was commandeered by a Russian cybergang. This is bad since MICROS is in the top three most popular payment systems in the world.

In a statement to Gizmodo, Oracle said it had detected and addressed malicious code in certain legacy MICROS systems. Right now, the extent of the breach is unclear, and the damage inflicted by the hackers has yet to be determined.

Krebs spoke with two security experts who have been breached on Oracle s investigation, who drew a connection to Russian hackers. From Krebs:

Oracle s MICROS customer support portal was seen communicating with a server known to be used by the Carbanak Gang. Carbanak is part of a Russian cybercrime syndicate that is suspected of stealing more than $1 billion from banks, retailers and hospitality firms over the past several years.

The hackers were reportedly able to steal all of the username and passwords of anyone who logged onto the MICROS support website after they had placed malicious code on the website. Oracle says that this hack hasn t put any credit card or payment data at risk, but the company did force all MICROS users to reset passwords for the MICROS support terminals.

Again, MICROS is a vey popular point of sale system, with over 330,000 point of sale terminals. But it s unclear how many of those terminal users logged into the support website. When reached by Gizmodo, an Oracle representative declined to comment, but said that he was aware of the report by Krebs On Security.

Data Breach   Oracle’s Micros Payment Systems Hacked

The risks associated with data breaches continue to grow, impacting a variety of industries, tech firms, and social networking platforms. In the past few months, over 1 Billion credentials were dumped online as a result of mega breaches in popular social networks.

Now, Oracle is the latest in the list.

Oracle has confirmed that its MICROS division   which is one of the world’s top three point-of-sale (POS) services the company acquired in 2014   has suffered a security breach.

Hackers had infected hundreds of computers at Oracle’s point-of-sale division, infiltrated the support portal used by customers, and potentially accessed sales registers all over the world.

The software giant came to know about the data breach after its staff discovered malicious code on the MICROS customer support portal and certain legacy MICROS systems. Hackers likely installed malware on the troubleshooting portal in order to capture customers’ credentials as they logged in.

These usernames and passwords can then be used to access their accounts and remotely control their MICROS point-of-sales terminals.

In a brief letter sent to MICROS customers, Oracle told businesses to change their MICROS account passwords for the MICROS online support site   particularly passwords that are used by MICROS staff to control on-site payment terminals remotely.

"Oracle Security has detected and addressed malicious code in certain legacy MICROS systems," said the company. "Oracle’s Corporate network and other cloud and service offerings were not impacted by this code."

"Payment card data is encrypted both at rest and in transit in the MICROS hosted environment Consistent with standard security remediation protocols, Oracle [requires] MICROS customers to change the passwords for all MICROS accounts."

Citing unknown sources, security news site KrebsOnSecurity, reported that the attack possibly came from a Russian crime gang, dubbed Carbanak Gang, that has been accused of stealing more than $1 Billion from banks and retailer stores in past hacks.

Sounds From Your Hard Disk Drive Can Even Be Used To Steal A PC’s Data

Researchers have found a way to steal a PC s data by using the mechanical noise coming from the hard disk drives inside.

It s not a very practical hack, but the scheme has been designed for air-gapped systems, or computers that have been sectioned off from the Internet.

The researchers at Ben-Gurion University of the Negev in Israel have been studying how to use sound to extract information from air-gapped computers. In June, they showed that even a PC s cooling fans can be controlled to secretly transmit data, including passwords and encryption keys.

In a new paper, the researchers found that a PC s hard disk drive could also generate enough noise to do the same. They did this, by manipulating the drive s internal mechanical arm, to generate binary signals.

Typically, the mechanical arm only reads and writes data within the hard drive. But when in use, it also creates a good deal of sound at different frequencies - which the researchers decided to exploit.

They developed a piece of malware called DiskFiltration which can infect a Linux-based PC to control a hard disk drive s operations. To record the emitted noise, the researchers placed a Samsung Galaxy S4 phone nearby to log and decrypt the signals.

They found that their hack could transmit enough 0s and 1s for a stream of data, including passwords. However, the transmission rate is quite slow at only 180 bits per minute, and the range is only effective at up to six feet.

Nevertheless, the method is covert. A hacker could infect an air-gapped system with a USB stick, and then secretly extract the data, by simply recording the nearby sounds.

To prevent this kind of hacking, owners of air-gapped owners can consider using solid-state drives, which have no moving parts, the researcher said.

New Hack Uses Hard Drive’s Noise To Transfer Stolen Data from Air-Gapped Computer

Air-gapped computers that are isolated from the Internet and other computers are long considered to be the most secure and safest place for storing data in critical infrastructures such as industrial control systems, financial institutions, and classified military networks.

However, these systems have sometimes been targeted in the past, which proves that these isolated systems are not completely secure.

Previous techniques of hacking air gap computers include:

AirHopper that turns a computer’s video card into an FM transmitter to capture keystrokes;
BitWhisper that relies on heat exchange between two computer systems to stealthily siphon passwords or security keys;
Hacking air-gapped computer using a basic low-end mobile phone with GSM network; and
Stealing the secret cryptographic key from an air-gapped computer placed in another room using a Side-Channel Attack.

Now, researchers have devised a new method to steal data from an infected computer even if it has not been physically connected to the Internet for preventing the computer to leak sensitive information stored in it.

Primary Focus of the ’DiskFiltration’ Research:

Ignoring the fact that how an air-gapped computer got infected with malware in the first place, the new research focused on, once infected, how the malware would be able to transfer data (passwords, cryptographic keys, keylogging data, etc.) stored on an air-gapped computer, without network, the Internet, USB port, Bluetooth, speakers, or any electronic device connected to it.

A team of researchers from Ben-Gurion University published their finding in a paper titled, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise," explaining a unique technique that uses acoustic signals (or sound signals) emitted from the hard disk drive (HDD) of the targeted air-gapped computer to transfer the stolen data.

You might have felt something spinning and generating weird noise while your computer reads or writes data on a storage hard drive.

That s the voice coil "actuator" inside your hard drive, which moves on the disk plate while accessing specific parts/blocks of the storage.

As demonstrated, the researchers used their malware to manipulate the movements of the actuator in very specific way to generate acoustic noise that they interpreted into binary data using a smartphone app from six feets away, at a speed of 180 bits per minute, Ars reported.

"The idle acoustic noise emitted from disk rotation is static and cannot be controlled by software," the paper explains.

"In order to modulate binary data, we exploit the seek acoustic noise generated by the movements of the actuator. By regulating (starting and stopping) a sequence of seek operations, we control the acoustic signal emitted from the HDD, which in turn can be used to modulate binary 0 and 1."

According to the paper, this technique is fast enough to transmit a 4,096-bit key within 25 minutes through manipulated sound signals emitted from the hard disk drive.

It s evident that in real-world situations, this technique is useless until we do not have an effective way to install malware remotely on an air-gapped computer at the first place, or an insider to help an attacker to get malware installed on the targeted computer using a USB.

As a workaround, researchers advised to replace the HDDs (Hard Disk Drives) with SSDs (Solid State Drives) to eliminate the DiskFiltration-style threat, since SSDs are not mechanical, thus generating virtually no noise.

Making use of a particularly quiet type of hard drives or installing the hard drives within special enclosures can also limit the range of emitted noise. Another countermeasure is to jam hard-drive signals by generating static noise in the background.

At the software and firmware level, making use of hard drives that includes automatic acoustic management (AAM) feature could also help in limiting the emitted acoustic noise.

Another solution is to ban smartphones and other types of recording devices nearby of the sensitive air-gapped computers.

Blackhat Firm Offers $500,000 for Zero-day iOS Exploit; Double Than Apple s Highest Bounty

Last week, Apple finally announced a bug bounty program for researchers and white hat hackers to find and get paid for reporting details of zero-day vulnerabilities in its software and devices.

The company offers the biggest payout of $200,000, which is 10 times the maximum reward that Google offers and double the highest bounty paid by Microsoft.

But now Apple is going to face competition from a blackhat company named, Exodus Intelligence.

Exodus Intelligence is offering more than double Apple’s maximum payout for zero-day vulnerabilities affecting the newest versions of iOS.

The company is willing to pay more than $500,000 for zero-day vulnerabilities and exploits affecting iOS 9.3 and above.

Although Exodus labeled itself as Research Sponsorship Program, the company actually makes money by buying and selling zero-day vulnerabilities and exploits.

On Wednesday, Exodus launched its new bonus structure for the acquisition of details and exploits for zero-day vulnerabilities.

Zero-Day Hit-list:

Exodus Intelligence’s hit-list also shows that the firm will pay:

Up to $150,000 for a zero day in Google Chrome (which is 50% more than the Google’s highest payout)
Up to $125,000 for a serious flaw in Microsoft’s Edge browser (which is $500 and $1,500 currently offered by Microsoft)
Up to $80,000 for a serious flaw in Mozilla’s Firefox.
Up to $75,000 reward for a local privilege escalation vulnerability in Windows 10
Also, Smaller payouts of $60,000 for flaws in both Adobe Reader and Flash Player

The zero-day market has long been a lucrative business for private companies that regularly offer more payouts for vulnerabilities than big technology firms.

Last year, security firm Zerodium paid $1 Million to a group of hackers for an iPhone hack, though that figure was later lowered to "up to $500,000" for subsequent iOS exploits.

The market for zero-day and exploits has become strong because governments, law enforcements, criminals, and the private sector shop for zero-days for surveillance or research purposes.

The well-known example is the latest fight between Apple and the FBI, which came to end when the FBI reportedly paid over $1 Million for an iPhone exploit that helped the FBI to break into the iPhone of one of the San Bernardino shooters.

There’s one more thing Apple should be worried about: While Apple s bug bounty program is invitation-only, at least for the time being, anyone can register on Exodus s website and participate in the program to submit vulnerabilities.

Don’t Baby These Kid Hackers

Emmett Brewer is no taller than the lectern on the stage, so he stands to the side of it to deliver his presentation. He’s got a Dennis the Menace hairdo and he’s only 10 years old, but I strongly suggest you take him seriously.

The topic of his speech today: hacking competitions. He’s showing other kids here how to run a capture the flag competition so their friends can learn new skills and trade secrets of how to bend software to their small but mighty wills.

That’s right, I’m in a room full of kid hackers. They range from the tiny to high school aged, and they want to learn how to break all the things.

"I like hacking, sniffing, jailbreaking, fuzzing - all that stuff," Emmett tells the room.

This is r00tz Asylum, a kid-centric event at the annual Defcon hacking event in Las Vegas. It started as a place for kids to hang out with parents instead of at the more mature talks going on down the hall, and over six years it has grown into a full-fledged hacking convention for kids.

In a ballroom at the Paris Resort, kids sit at tables on two sides of the room learning to pick locks and solder circuit boards. In another corner, a hacking competition like the one Emmett described in his talk is taking place. And on the stage, speakers talk frankly about the fun - and risks - of hacking.

"Do you want to do more lock picking?" asks a woman leading a tired-looking kindergarten-age boy.

"No," he says vaguely and wanders off to the part of room where the soldering is happening.

The conference this year involves the most presentations ever given by kids, including Emmett’s. His dad, Joel Brewer, got him interested in learning how to set up a hacking competition called capture the flag using a ready-to-use platform designed by Facebook.

Emmett Brewer explains how to use a platform created by Facebook for designing hacking competitions at the r00tz Asylum kids’ hacking event in Las Vegas.
Laura Hautala

"It was kind of exciting, but I was a little nervous," Emmett, who is starting the fourth grade in Austin this fall, says after giving his talk. Asked if he has any favorite subjects at school other than the computer lab, he says, "Nothing besides computer lab and recess." Now, he’s soldering together a circuit board that will eventually become an electronic game of Simon Says.

Facebook made its capture the flag platform open to the public this May. There was too much demand for it from schools and other child-focused organization for the company’s engineers to keep up with, said Javier Marcos, who as a Facebook cybersecurity specialist helped develop the competition platform but now works at Uber.

If you’re wondering why schools are teaching kids to hack and think these kids are future criminals, you’ve got it backward. Sure, young people do get in trouble for illegal hacking, but Facebook hopes it’s helping to train the cybersecurity experts of the future.

"We started running these CTF competitions as a way to find candidates," Marcos said. Now in addition to urging universities to host the competitions, they’ve helped a group of high school kids from Utah and Idaho put on the r00tz Asylum capture the flag using their platform.

This was a huge opportunity for Connor Jones, a 14-year-old who starts the ninth grade in Saratoga Springs, Utah, this fall. When he first talked with organizers from Facebook on the phone, he couldn’t believe it.

"Facebook is on the phone, and I’m like freaking out," he says. "It was really cool."

He and the other students involved with the project worked for the first half of their summer vacation coming up with the hacking challenges that made up the game. Connor loved every second of it, waking up at 8 a.m. every day and sitting in a rocking chair in his basement working on the different parts of the competition.

He thinks he’ll work in cybersecurity going forward. "I want to get out there and learn new things every day," he said.

After the children’s speeches are over, cybersecurity expert Dan Kaminsky takes the stage. Just four days earlier, Kaminsky gave the keynote speech to a vast ballroom full of adult cybersecurity experts at the Black Hat conference, another cybersecurity event that traditionally takes place in Las Vegas just before Defcon. Now, he’s facing a tough crowd of squirmy kids.

"Go ahead, break stuff," he tells the room. "That’s how I got where I am."

But, he says, that’s not all there is to hacking. Software affects people everywhere in the world now, so what they do next after finding problems in computer code matters.

"You’re going to be able to make things better," he concludes. He’s almost drowned out by the buzz of happy children picking locks, soldering circuit boards and hacking software.

Google To Push Flash Closer to Extinction With New Version of Chrome

Google plans to begin pushing Adobe Flash Player closer to its inexorable grave at the end of the year with a new version of its Chrome web browser.

Chrome 55, which the web giant plans to release in December, will replace Flash with HTML5, Google said on Monday. Noting that the browser plug-in has played a key role in the proliferation of video on the internet, Google said the change will lead to improved security, reduced power consumption and faster page load times.

"HTML5 is much lighter and faster, and publishers are switching over to speed up page loading and save you more battery life," Anthony LaForge, curator of Flash in Chrome, wrote in a blog post. "You’ll see an improvement in responsiveness and efficiency for many sites."

Google said it will begin to de-emphasize Flash in September with the release of Chrome 53, which will begin blocking the plug-in.

Adobe responded to the move by reiterating that it believes HTML5 is the web platform of the future.

"We work closely with Mozilla, Microsoft, Facebook and others to facilitate the adoption of these open standards," Adobe said in a statement. "Google’s decision is part of this industrywide evolution that Adobe is heavily invested in."

Once the de facto standard for websites to run games, stream video and deliver animation over browser software, Flash Player has fallen out of favor with many tech companies and organizations, which deride the plug-in as a battery hog and security vulnerability. Its popularity has waned in recent years as more in the online video industry turn to HTML5, a developing language that can run graphics without plug-ins.

We Need More High-speed Internet,
But Politicians Are Blocking The Way

It s been a rough few days for people looking for alternatives to their current internet providers.

Last week, the Federal Communications Commission issued a report documenting what many of you already know: You don t have much choice when it comes to broadband. In fact, most of you have only one or no companies selling high-speed internet. Then on Wednesday, a court ruling held the FCC can t override state laws restricting cities and towns from launching their own broadband services to increase their residents provider options.

Neither development should have been that much of a surprise.

The FCC s Internet Access Services: Status as of June 30, 2015 report, released Aug. 5, leads off with the reassuring news that our download speeds are getting faster. Of the 91 million residential wired connections counted as of last June 30, just over half 52% hit at least 25 megabits per second (Mbps), the minimum download speed the FCC considers to be broadband. Another 25% ranged between at least 10 Mbps to just below 25 Mbps.

Connections between 3 Mbps and less than 10 Mbps, what amounts to entry-level broadband these days, constituted 17% of the total, and sub-3 Mbps service added up to 6%. The report, based on data broadband providers reported to the FCC, excluded connections slower than 200 kilobits per second.

Unfortunately, many Americans don t have much choice when it comes to selecting broadband providers in their areas. The FCC found that while 75% of Census blocks (the smallest demographic unit the Census Bureau counts) had three or more 3-10 Mbps residential providers and 63% had three or more 10-25 Mbps providers, just 3% offered at least three broadband sources with speeds of 25 Mbps or faster. That last figure was unchanged from the FCC s mid-2014 data.

In that 25-Mbps-and-up range, 48% of Census blocks had only one provider available, 30% had none and only 22% had two options.

It s not all bad news, though. According to a 2010 report, only 4% of Census tracts had three or more internet providers selling at least 4 Mbps service. We re definitely doing better than that.

The FCC s latest report indicates that cellular connections vastly outnumbered wired access   they made up 68.8% of total residential connections   but those come with data caps that make them unusable as a primary connection for most home users.

The FCC report also underscored the dominance of cable, which constituted 59% of residential wired connections. Slower phone-based digital subscriber lines had second place at 28%, and fast fiber-optic service   the only technology out of those three to offer upload speeds generally as fast as download speeds   was third at 10%.

Some speed-starved cities and towns have considered getting into the broadband internet business themselves. But that won t work if their states prohibit them from offering municipal broadband or chain any such ventures down with restrictions that make them unviable.

About 20 states have done just that. As a 2015 Pro Publica report outlined, generous campaign contributions from telecom firms to state-level candidates ($870,000 in North Carolina, $921,000 in Tennessee) helped that happen.

Two cities with muni broadband services constrained from expansion by state laws   Chattanooga, Tenn., and Wilson, N.C. asked the FCC to override those bans. In February 2015 the commission voted to do so in the same meeting that saw the adoption of sweeping net-neutrality regulations.

And just like those better-known rules, which ban Internet providers from slowing websites and services or charging a site for faster delivery, the FCC s preemption of North Carolina and Tennessee laws quickly drew a court challenge. But while the FCC won the net-neutrality case, it lost the municipal-broadband decision.

A three-judge panel at the United States Court of Appeals for the Sixth Circuit held that the FCC had no authority to knock down state muni-broadband limits. The commission s move, Judge John M. Rogers wrote in the court s opinion, requires at least a clear statement in the authorizing federal legislation   and the provision of the Telecommunications Act of 1996 that the FCC cited falls far short of such a clear statement.

I can t say that surprised me. Tech-policy types who favor muni broadband thought last year that this preemption was riskier than the net-neutrality rules, which relied on a more specific branch of telecom law.

Rogers was careful to note the appeal of services like Chattanooga s EPB, which charges $69.99 for 1 Gbps, and Wilson s Greenlight, which sells the same speed for $99.95. The former led to job growth and attracted businesses to the area, pushed competing providers to cut their rate and made money for the city, while the latter also turned a profit and has won the business of the top seven employers in Wilson.

(A study released last month by Tennessee s economic-development department about the state s broadband needs endorsed the potential of community broadband and suggested ending the state s restrictions on it.)

Now what?

Alas, neighbors of these two cities will have to wait longer to get such fast internet speeds at those rates. FCC chair Tom Wheeler conceded as much in a statement saying the ruling appears to halt the promise of jobs, investment and opportunity that community broadband has provided in Tennessee and North Carolina.

A longtime advocate of municipal broadband was a little more hopeful. We are better off for the FCC having pushed this hard to encourage competition, said Christopher Mitchell, who runs the Institute for Local Self-Reliance s community-broadband initiative. He pointed to the incredible record of muni-broadband success now in the public view.

But the court s ruling now makes it clear that help for this won t come from Washington. People in states like North Carolina and Tennessee will either need to elect some new state representatives or get their current legislators to pay less attention to Big Telecom. Either way, we may be looking at a longer download time for a better choice in broadband.

On This Day 25 Years Ago, The World’s First Website Went Online

On this day 25 years ago, August 6, 1991, the world’s first website went live to the public from a lab in the Swiss Alps.

So Happy 25th Birthday, WWW! It’s the Silver Jubilee of the world’s first website.

The site was created by Sir Tim Berners-Lee, the father of the World Wide Web (WWW), and was dedicated to information on the World Wide Web project.

The world’s first website, which ran on a NeXT computer at the

European Organization for Nuclear Research (CERN), can still be visited today, more than two decades after its creation.

The first website address is http://info.cern.ch/hypertext/WWW/TheProject.html.

"The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents," the world’s first public website reads, going on to explain how others can also create their own web pages.

"The project started with the philosophy that much academic information should be freely available to anyone."

Berners-Lee wrote about the HyperText Transfer Protocol (HTTP) that outlined how information or data would travel between computer systems, as well as, HyperText Markup Language (HTML) that was used to create the first web page.

Berners-Lee vision was to create a place where people could share information across the world through a "universal linked information system" in which a network of documents (web pages) linked to one another could help users navigate to find what exactly they need.

And so is the concept of the World Wide Web.

Berners-Lee initially proposed the idea for a worldwide network of computers sharing information in 1989, while he was working as a computer programmer at the European Organization for Nuclear Research (CERN) in Geneva, Switzerland.

The World Wide Web was written on a NeXT computer, made by the company Steve Jobs founded after he was kicked out of Apple back in 1985.

"We bought a cool machine, the NeXT computer," Berners-Lee said two years ago during an interview at Rensselaer Polytechnic Institute. "NeXT was a machine made by Steve Jobs when he was kicked out of Apple [in 1985]... it had a wonderful spirit to it, a really good developer’s environment."

"When you opened it, you got a pre-recorded message from Steve that said, ’Welcome to the NeXT. This is not about personal computing. It’s about ’inter-personal’ computing.’ It was perfect for designing the web."

The website went live to the public on August 6, 1991; that’s exactly 25 years back. At the time, Berners-Lee taped a note to the front of his NeXT computer, saying:

"This machine is a Server. DO NOT POWER DOWN."

When Berners-Lee created the World Wide Web, his idea was simply to create a tool for scientists to find and share information with ease.

The Web has since become the world s most powerful medium for knowledge, communications, and trade   but that doesn’t mean he is happy with all of the consequences.

Last month, Berners-Lee turned 61 and regretted a lot of things about his invention. He has primarily concerned that the Internet has now transformed into the "world’s largest surveillance network."

Today, the Web "controls what people see, creates mechanisms for how people interact," New York Times quoted Berners-Lee as saying. "It is been great, but spying, blocking sites, repurposing people’s content, taking you to the wrong websites that completely undermines the spirit of helping people create."

This is why the creator of the Internet is figuring out what the next step should be for the World Wide Web.

The Web model relies on central servers and IP addresses, which can easily be tracked or blocked. Therefore, Berners-Lee is looking to decentralize the whole Web, the report said.

"The web is already decentralized," he said. "The problem is the dominance of one search engine, one big social network, one Twitter for microblogging. We do not have a technology problem; we have a social problem."

The idea is simple:

To eliminate middleman completely from all aspects of the Web. Still, all the major players do not agree to this decentralize approach. It’s still a question that whether the Internet needs decentralizing.

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.